RSAC 2025 Conference

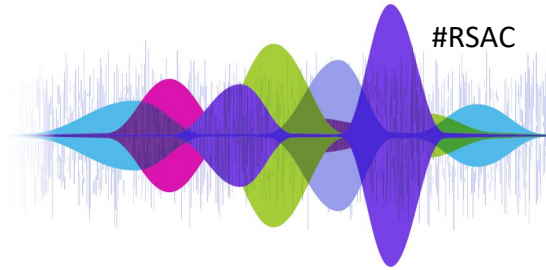
Many Voices.
One Community.

SESSION ID: CIT-R05

Choo-Choo Cybersecurity: A New Era

Arturo Santos

Director - Enterprise Cybersecurity Architecture - Amtrak
Secretary of the ANSI Technical Advisory Group for the IEC Technical Committee for Rail Applications
Board member of the cybersecurity group of the American Public Transportation Association - APTA



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Who Is This Presentation For?

- Anyone working in the rail industry or critical infrastructure supply chain
  - Rail operators
  - Service providers
  - Maintenance organizations
  - Auditors and inspectors
  - Federal, State and local partners sharing the infrastructure
- Anyone dealing with cybersecurity frameworks and protection requirements for critical infrastructure
- Anyone interested on how international standards are developed and implemented

Anyone who rides a train, tram, metro, local commuter anywhere in the world

Rail is Critical Infrastructure!!

- Trivia question: Can you name 5 countries without any form of rail transportation?
- Everyday 8 Billion passengers/km and 33 Billion tons/km are transported across 1.5 million km of railways worldwide
- Cyber-physical devices, collect, analyze and act on terabytes of data transmitted over internet and clouds from critical systems for traffic management, train control, diagnostics, and maintenance.
- Sophistication comes at a cost: Recent accidents can be traced to automated actions based on corrupted or incomplete data

Rail Cyber Security
Overview, Background, Evolution

- The current and evolving cyber threat landscape to rail
- Background on TC9
- Background on IEC 63452 Working Group
- US delegation role in the development of the standard
- The applicability and scope of the standard
- IEC 63452 as an enabler to achieve compliance

IEC Cybersecurity Standard for Rail Applications

Goal: Build a comprehensive framework to enhance rail security, based on *existing* cybersecurity standards including IEC 62443 & TS 50701, for all railway networks including passenger, freight, metros, trams, trolleys, high speed and levitated transport

RAILWAY CYBERSECURITY IEC 63452

Developed by the International Electrotechnical Commission (IEC), Technical Committee 9, under the project PT 63452, by 143 experts in 4 Continents, representing 23 countries.

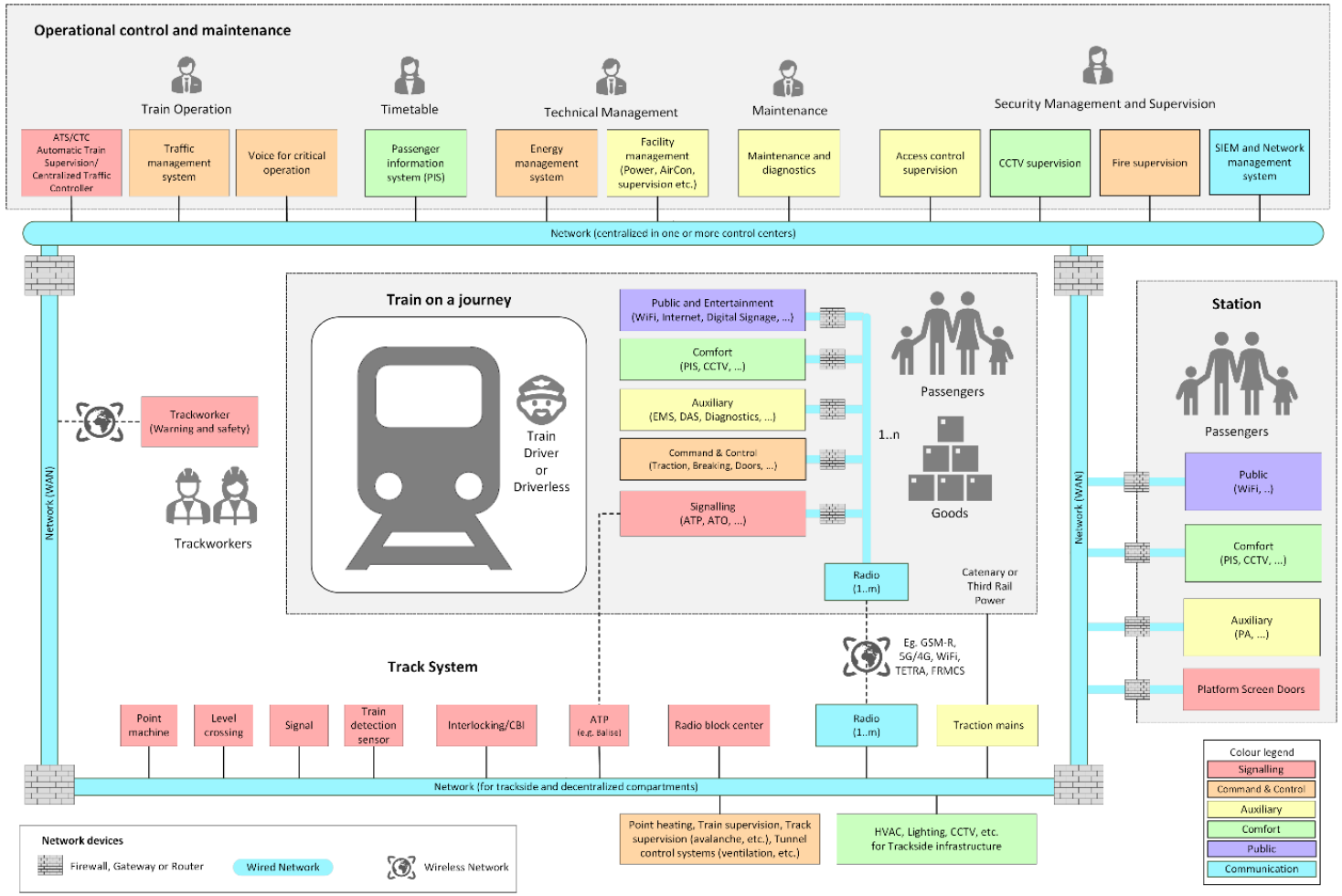
US Priorities:

1. Define clear guidelines and best practices to mitigate cybersecurity risks in an increasingly connected rail environment.
2. Ensure the United States rail cybersecurity position is considered within the international standard
3. Build partnerships as the standard is developed and implemented across the rail industry

US Accomplishments:

- ✓ Technical recommendations for updating the standard
- ✓ Editorial revision for English language grammar and style
- ✓ Include input with federal partners on security interests
- ✓ Coordinating industry peers and state partners
- ✓ Engaging US operators and suppliers

Rail Systems / Functional Requirements



- FR 1: Identification and authentication control (IAC)
- FR 2: Use control (UC)
- FR 3: System integrity (SI)
- FR 4: Data confidentiality (DC)
- FR 5: Restricted data flow (RDF)
- FR 6: Timely response to events (TRE)
- FR 7: Resource availability (RA)

RAILWAY CYBERSECURITY IEC 63452

RSAC™ 2025 Conference

IEC 63452 Overview

Collaborating With a Common Understanding

- Purpose
- Scope
- Vocabulary
- Railway System Overview

IEC 63452 Overview

- Enterprise Cybersecurity Management
- Cybersecurity within a railway application life-cycle
- Zone and risk assessment
- Cybersecurity architecture
- Cybersecurity assurance
- Operational Maintenance and Decommissioning

RAILWAY CYBERSECURITY IEC 63452

Enterprise Cybersecurity Management

- Establish a railway OT cybersecurity policy and program
  - Establish high-level objectives
- Focus areas:
  - Risk Management
  - Asset Management
  - Supply Chain Management
  - Skills development
- Business Continuity
- Alignment with overall policies and business strategies

Cybersecurity Within a Railway Application Life-cycle

The asset owner / system integrator project cybersecurity managers are responsible for developing and maintaining the cybersecurity management plan, ensuring its effective application by monitoring the implementation of the related cybersecurity activities. The maintenance service provider project cybersecurity manager is responsible for developing and maintaining the cybersecurity maintenance plan

Zoning and Risk Assessment

- "It is assumed that for railway applications, a detailed risk assessment is almost always necessary."
- Specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) should guide functional and architectural description of the System Under Consideration (SUC).
- Cybersecurity context -> Initial risk assessment
- Use "zones and conduits" model with appropriate criteria (e.g. risk, safety, etc.)
- Detailed risk assessment including identification of threats, vulnerabilities, explicit risk evaluation of unmitigated risk
- Asset owners will make decisions to accept risk

Cybersecurity Architecture

- Defined SUC functional cybersecurity architecture
- Cybersecurity requirements apportioned to each zone, conduit and sub-systems within the SUC
- SUC cybersecurity parameters and configuration management system
- Guidelines for the operation and maintenance of the cybersecurity functions within the SUC
- Cybersecurity architecture, apportionment of security requirements and integration
- Cybersecurity guidelines for the railway solution
- **Cybersecurity shall not adversely impact essential functions**

Cybersecurity Assurance

- Activities performed throughout the development of the railway solution, which culminate in its acceptance by the asset owner at handover.
- Major inputs to the activities of Cybersecurity assurance
  - cybersecurity requirements specification (CRS)
  - all identified security-related application conditions (SecRACs)
- Cybersecurity Evaluation plan is required and will include verification evidence
- Railway solution acceptance
  - Cybersecurity handover plan and report

RAILWAY CYBERSECURITY IEC 63452

Operational, Maintenance and Decommissioning

- Create a Cybersecurity Maintenance plan highlighting
  - Continuous verification
  - Risk assessment updates including
    - Vulnerability Management
    - Patch Management
  - Incident Management
  - Security monitoring
  - Decommissioning

RAILWAY CYBERSECURITY IEC 63452

RSAC 2025 Conference

Annexes

IEC 63452 Annexes

- Handling conduits
- Handling legacy systems
- Cybersecurity design principles and system requirements
- Safety and cybersecurity
- Risk acceptance methods
- Railway system models and zone models
- Cybersecurity deliverables content
- Cybersecurity roles and competence profiles
- Cybersecurity for operation and maintenance activities – operational guidance
- Vulnerability management – operational guidance
- Cloud Security

RAILWAY CYBERSECURITY IEC 63452

Cloud Security

Applies solely to cloud implementations of the railway solution, devices, applications, data, technology resources and digital assets directly involved in the control, monitoring, and operation of rail infrastructure and rolling stock

RAILWAY CYBERSECURITY IEC 63452

Handling Conduits

- Conduits are links/channels between zones. Three types
  - Transparent
  - Filtering
  - Unidirectional
- Protection profiles for conduits

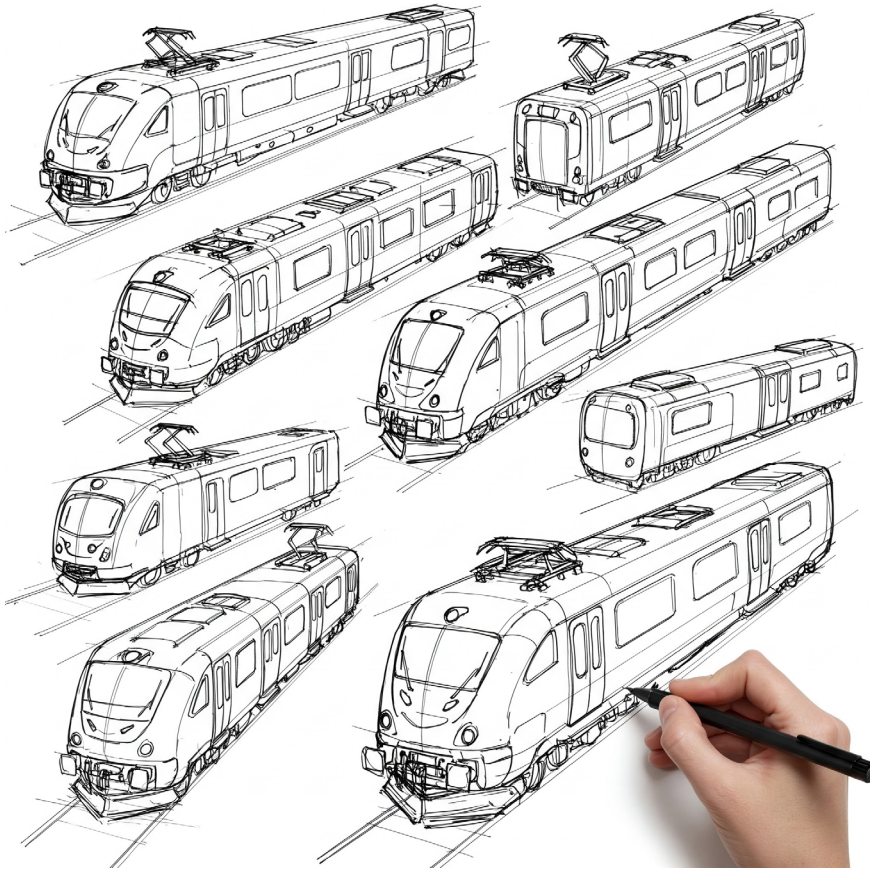
Handling Legacy Systems

Defines the technical and organizational countermeasures to achieve a minimum security level for systems that cannot meet a IEC 62443 security level

RAILWAY CYBERSECURITY IEC 63452

Design Principles and System Requirements

- Various concepts explained
  - Fail secure
  - Least privilege
  - Authentication
  - Access control
  - Privacy
  - Auditing and monitoring



RAILWAY CYBERSECURITY IEC 63452

Safety and Cybersecurity

- Clarifies the distinction between safety and security
- Co-engineering safety and security
- The relationship between safety integrity levels and security levels

RAILWAY CYBERSECURITY IEC 63452

Railway System and Zone Models

- Design guidance for system and zone models are provided
- Several use cases are provided to aid in defining zone criticality

Deliverables Content

- OT cybersecurity policy
- OT cybersecurity program
- Cybersecurity maintenance plan
- Railway application cybersecurity case
- Cybersecurity management plan
- Cybersecurity risk assessment report
- Cybersecurity requirement specification
- Cybersecurity evaluation plan
- Cybersecurity guidelines
- Railway solution cybersecurity case

Roles and Competence Profiles

- Describes competency profiles for 11 cybersecurity roles in the railway applications lifecycle
- Tailored from the European Cybersecurity Skills Framework (ECSF)
- Represents activities that should be performed, but does not impose project team sizes

Risk Acceptance Methods

- Examples of risk assessment methods are provided
- Covers a range of use cases that may be useful to system integrators, turn-key suppliers, infrastructure managers, and product suppliers

Vulnerability Management – Operational Guidance

- Process scoping
- Vulnerability analysis and prioritization criteria
- Vulnerability remediation

RAILWAY CYBERSECURITY IEC 63452

Cybersecurity for Operations & Maintenance Activities – Operational Guidance

- Early engagement with maintenance teams
- Physical security
- Role-based access
- Remote access and maintenance

RAILWAY CYBERSECURITY IEC 63452

RSAC™ 2025 Conference

Next Steps

Many Voices.
One Community.

Next Steps

- IEC 63452 to be published in late 2025 but you can start adopting today!!
- Raise awareness!
  - Discuss internally and within cybersecurity and industry forums
    - American Public Transportation Association (APTA)
    - Federal Transit Administration (FTA)
    - Transportation Security Administration (TSA)
    - NIST's National Cybersecurity Center of Excellence (NCCoE)
  - Engage more operators, vendors, state and city partners
- Help map IEC 63452 controls with TSA, NIST, FRA requirements

RSAC 2025 Conference

Many Voices.
One Community.

Thank You!!

Arturo Santos